GEORGIA SOUTHERN UNIVERSITY

PROTECTION AND SECURITY OF DATA AND INFORMATION

Area:	Information Technology	Number:	
Applies to:	University Community	Issued:	October 15, 2010
Sources:	See 'Relevant Documents' at the end of this policy	Revised:	May 18, 2020
		Reviewed:	
Policy Owner:	Chief Information Officer	Page(s):	4

I. Purpose

Data and information are valuable assets owned by the University. The Board of Regents of the University System of Georgia Business Procedures Manual establishes that all institutional data is to be used with appropriate and relevant levels of access and with sufficient assurance of its security and integrity in compliance with existing laws, rules and regulations. As such, each institution has a responsibility to protect the confidentiality, integrity, and availability of data and information generated, accessed, modified, transmitted, stored or used by the University, on any medium on which the data resides and regardless of format.

II. Policy Statement

All employees and contractors who are granted authorization to access the University's data and information assets have a responsibility to protect those assets from unauthorized access, destruction, disclosure, generation, modification or transmission; and are expected to be familiar with and comply with University System procedures for protection and security of records. All data stored on University resources or other resources where University business occurs must be appropriately identified according to Data Stewardship and Classification Standards as established by the Chief Information Officer.

The Gramm-Leach-Bliley Act (GLBA) mandates that the University appoint an Information Security Program Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, review service providers prior to adoption, and evaluate and adjust the Information Security Program periodically. The Chief Information Officer (CIO) delegates this authority to the Chief Information Security Officer (CISO).

III. Definitions

Covered Data and Information includes student information that is protected under the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA), European Union General Data Protection Regulation (EU GDPR), the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI DSS), etc. Georgia Southern University chooses, as a matter of policy, to include in this definition any and all sensitive and/or

personally identifying data, including credit card information and checking/banking account information received in the course of business by the University, whether or not such information is covered by federal statutes. Covered data and information include both paper and electronic records.

IV. Exclusions

These are no exclusions or exceptions to the policy.

V. Procedures

Violation of this policy can lead to disciplinary action up to and including dismissal, and/or legal action.

A. Identification and Assessment of Risks to Customer Information

Georgia Southern University recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access to covered data and information by someone other than the owner of the covered data and information.
- Compromised system security as a result of system access by an unauthorized person.
- Interception of data during transmission.
- Loss of data integrity.
- Physical loss of data in a disaster.
- Errors introduced into the system.
- Corruption of data or systems.
- Unauthorized access to covered data and information by employees.
- Unauthorized requests for covered data and information.
- Unauthorized access through hardcopy files or reports.
- Unauthorized transfer of covered data and information through third parties.

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information, and that new risks are created regularly, Georgia Southern University Office of Cyber Security will actively participate and monitor appropriate cybersecurity advisory groups for identification of risks. Risk assessments will allow the Office of Information Security to:

- Ensure the security and confidentiality of covered data and information;
- Protect against anticipated threats or hazards to the security or integrity of such information;
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.
- Identify and assess the risks that may threaten covered data and information maintained by Georgia Southern University;
- Develop written policies and procedures to manage and control these risks;
- Adjust the program to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

B. Employee Management and Training

References and/or background checks (as appropriate, depending on position) of new employees working in areas that regularly work with covered data and information (e.g. Bursar's Office, Financial Aid, Registrar's Office, Information Technology) are checked/performed as part of the employment process. During employee orientation, each new employee in these departments receives proper training on the importance of confidentiality of student records, student financial information, and all other covered data and information. Each new employee is also trained in the proper use of computer information and passwords. This training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. These training efforts are provided to help minimize risk and safeguard covered data and information.

C. Physical Security

Georgia Southern University limits access to covered data and information to only those employees who have a legitimate business reason to handle such information. Each department must assign an individual who is responsible for maintaining covered data and information from damage due to environmental hazards, such as fire and water damage or technical failures, as defined by this policy.

D. Information Systems

Access to the University's information systems is limited to those employees who have a legitimate business reason to access such information. The University has policies and procedures in place to complement the physical and technical safeguards in order to provide security to Georgia Southern's information systems. (See list of Relevant Documents at the end of this policy.) These policies and procedures are maintained by the Chief Information Security Officer.

E. Management of System Failures

Georgia Southern's Office of Information Security has developed a written Incident Response Plan which outlines procedures for responding to unauthorized access to covered data and information.

F. Oversight of Service Providers

Federal regulations, including GLBA, FERPA, HIPAA, PCI DSS, and EU GDPR require the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. The University ensures that such steps are taken by contractually requiring service providers to implement and maintain such safeguards. The Office of Information Security and the Office of Legal Affairs will review each service provider contract to ensure it contains appropriate terms to protect the security of covered data. Each department is responsible for notifying the Office of Legal Affairs when a contract includes sharing covered data and information with a vendor.

G. Continuing Evaluation and Adjustment

This Policy will be reviewed annually.

VI. Related Documents

- GLBA Compliance: FTC website
- GLBA Compliance: Educause website
- FERPA – US Department of Education website
- PCI DSS
- Digital Commons
- Data Stewardship and Classification Standards
- Information Technology Acceptable Use Policy
- FERPA Policy